AMENDMENTS TO THE CLAIMS:

The listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

Claims 1-96 (canceled).

97.   (New) A data structure embodied on a computer-readable medium, the data structure comprising:

information that identifies, at least in part, a first digital object;

a first target data block, the first target data block specifying rights pertaining to the first digital object, the first target data block being written in a first format; and

a second target data block, the second target data block specifying rights pertaining to the first digital object, the second target data block being written in a second format, the second format being different from the first format.

98.   (New) A data structure as in claim 97, further comprising:

a first cryptographic seal, the first cryptographic seal having been created using a key associated with a creator of the data structure.

99.   (New) A data structure as in claim 98, further comprising:

a second cryptographic seal, the second cryptographic seal being associated with the first target data block; and

a third cryptographic seal, the third cryptographic seal being associated with the second target data block.

100. (New) A data structure as in claim 99, in which the second cryptographic seal and the third cryptographic seal are created using the key associated with the creator of the data structure.

101. (New) A data structure as in claim 100, in which the key comprises a private key of an asymmetric key pair.

102. (New) A data structure as in claim 101, further comprising:

a public key of the asymmetric key pair.

103. (New) A data structure as in claim 102, in which the public key is certified by a certifying authority.

104. (New) A data structure as in claim 101, in which the first cryptographic seal comprises an encrypted hash of at least part of the data structure, the hash being encrypted with the key.

105. (New) A data structure as in claim 104, in which the data structure further comprises a header, and the hash comprises a hash of at least part of the header.

106. (New) A data structure as in claim 100, in which the second cryptographic seal is created by encrypting a hash of at least part of the first target data block using the key associated with the creator of the data structure, and in which the third cryptographic seal is created by encrypting a hash of at least part of the second target data block using the key associated with the creator of the data structure.

107. (New) A data structure as in claim 106, in which the first target data block includes a header, and in which the hash of at least part of the first target data block comprises a hash of at least part of the first target data block's header.

108. (New) A data structure as in claim 107, in which the second target data block includes a header, and in which the hash of at least part of the second target data block comprises a hash of at least part of the second target data block's header.

109. (New) A data structure as in claim 97, further comprising:

a data structure identification number.

110. (New) A data structure as in claim 109, further comprising:

a first target data block identification number; and

a second target data block identification number.

111. (New) A data structure as in claim 110, in which the first data structure identification number, the first target data block identification number, and the second target data block identification number each comprise a unique identification number.

112. (New) A data structure as in claim 97, further comprising:

a third target block, the third target block specifying rights pertaining to the first digital object, the third target block being written in a third format, the third format being different from the first format and the second format.

113. (New) A data structure as in claim 97, in which the first target block and the second target block express at least some of the same rights.

-4-

23 114. (New) A data structure as in claim 97, in which the first target block is understandable by a first rights management environment, and the second target block is understandable by a second rights management environment that is unable to understand the first target block.

24 115. (New) A data structure as in claim 97, in which the first digital object comprises executable code.

25 116. (New) A data structure as in claim 97, in which the first digital object comprises at least one of: textual electronic content, audio electronic content, video electronic content, and graphical electronic content.

26 117. (New) A data structure as in claim 97, in which the data structure is machine readable.

18 118. (New) A data structure as in claim 113, in which the rights specify one or more permitted operations on the first digital object.

19 119. (New) A data structure as in claim 118, in which the rights further specify an authorized extent of the one or more permitted operations.

20 120. (New) A data structure as in claim 119, in which the rights specify a number of copies that may be made of the first digital object.

21 121. (New) A data structure as in claim 118, in which the rights further specify at least one consequence of performing the one or more permitted operations.

22 122. (New) A data structure as in claim 113, in which the rights specify one or more required operations on the first digital object.

27
~~123~~. (New) A data structure as in claim ~~97~~, further comprising:

information that identifies, at least in part, a second digital object.

28
~~124~~. (New) A data structure as in claim ~~123~~, further comprising:

a third target data block, the third target data block specifying rights pertaining to the second digital object.

29
~~125~~. (New) A data structure as in claim ~~123~~, in which the first target data block specifies rights pertaining to the second digital object, and in which the second target data block specifies rights pertaining to the second digital object.

30
~~126~~. (New) A computer program product embodied on a computer-readable medium, the computer program product including instructions which, when executed by a computer system in a first rights management environment, cause the system to perform actions comprising:

receiving a digital object;

receiving a data structure associated with the digital object, the data structure containing a first target data block and a second target data block, the first target data block being adapted for use in the first rights management environment, and the second target data block being adapted for use in a second rights management environment; and

enforcing at least one rule located within, or referenced by, the first target data block to control at least one use of said digital object.

-6-

31 127. (New) A computer program product as in claim 126, further including instructions which, when executed by a computer system in a first rights management environment, cause the system to perform actions comprising:

calculating a hash of at least part of the first target data block;

decrypting an encrypted hash value received in said data structure; and

comparing the calculated hash with the decrypted hash.

32 128. (New) A computer program product as in claim 126, further including instructions which, when executed by a computer system in a first rights management environment, cause the system to perform actions comprising:

evaluating a measure of trust associated with a source of said data structure,

wherein said action of enforcing at least one rule is selectively performed based at least in part on a result of said evaluating step.

33 129. (New) A data structure embodied on a computer-readable medium, the data structure comprising:

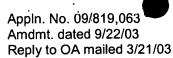information that identifies, at least in part, a digital object;

a first rule, the first rule specifying rights pertaining to the digital object;

a second rule, the second rule specifying rights pertaining to the object,

wherein the second rule specifies said rights using a different mechanism from the first rule.

-7-

34 130. (New) A data structure as in claim 33 129, further comprising:

a third rule, the third rule specifying rights pertaining to the object, the third rule specifying said rights using a different mechanism from the first rule and the second rule.

35 131. (New) A data structure as in claim 33 129, in which the first rule and the second rule express the same rights.

36 132. (New) A data structure as in claim 33 129, in which the first rule is interpretable by a first rights management system, and the second rule is interpretable by a second rights management system.

37 133. (New) A data structure as in claim 36 132, in which the first rights management system and the second rights management system employ substantially incompatible mechanisms for specifying rights pertaining to objects.

38 134. A rights management method comprising:

receiving a digital object in a first rights management environment;

receiving a data structure associated with the digital object, the data structure containing a first target data block and a second target data block, the first target data block being designed for use in the first rights management environment, and the second target data block being designed for use in a second rights management environment; and

enforcing at least one rule located within, or referenced by, the first target data block to control at least one use of said digital object,

-8-

wherein the first rights management environment defines rules pertaining to the use of objects in a manner that is substantially incompatible with the manner by which the second rights management environment defines rules pertaining to the use of objects.

39

135. A method as in claim 134, further comprising:

calculating a hash of at least part of the first target data block;

decrypting an encrypted hash value received in said data structure; and

comparing the calculated hash with the decrypted hash.

40

136. A method as in claim 134, in which the digital object and the data structure are received together.

41

137. A method as in claim 134, further comprising:

evaluating a measure of trust associated with a source of said data structure,

wherein said enforcing step is selectively performed based at least in part on a result of said evaluating step.

42

138. A method as in claim 134, in which the first rights management environment comprises a computer running a first rights management system, and in which the second rights management environment comprises a computer running a second rights management system.

78